UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

Joe Alves, individually and on behalf of all others similarly situated, Plaintiff, v. GOODYEAR TIRE AND RUBBER COMPANY, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

COMPLAINT - CLASS ACTION

Plaintiff Joe Alves ("Plaintiff"), individually and on behalf of all others similarly situated, hereby files this class action complaint against Defendant Goodyear Tire and Rubber Company ("Defendant" or "Goodyear"), and in support thereof alleges the following:

INTRODUCTION

1. This is a class action brought against Goodyear for wiretapping the personal and private electronic communications of visitors to its website, www.goodyear.com, without their consent. Goodyear procures and directs third-party vendors, such as Microsoft Corporation ("Microsoft"), to embed snippets of JavaScript computer code ("Session Replay Code") on Goodyear's website, which then deploys on each website visitor's internet browser for the purpose of intercepting and recording the website visitor's electronic communications with the Goodyear website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications

in real-time ("Website Communications"). These third-party vendors (collectively, "Session Replay Providers") create and deploy the Session Replay Code at Goodyear's request.

2. After intercepting and capturing the Website Communications, Goodyear and the Session Replay Providers use those Website Communications to recreate website visitors' entire visit to www.goodyear.com. The Session Replay Providers create a video replay of the user's behavior on the website and provides it to Goodyear for analysis. Goodyear's procurement of the Session Replay Providers to secretly deploy the Session Replay Code results in the electronic equivalent of "looking over the shoulder" of each visitor to the Goodyear website for the entire duration of their website interaction.

3. Goodyear's conduct violates the Massachusetts Wiretapping Act, Mass. Gen. Laws ch. 272, §99, the Massachusetts Invasion of Privacy Statute, Mass. Gen. Laws ch. 214, §1, and constitutes a general invasion of the privacy rights of website visitors.

4. Plaintiff brings this action individually and on behalf of a class of all Massachusetts citizens whose Website Communications were intercepted through Goodyear's procurement and use of Session Replay Code embedded on the webpages of www.goodyear.com and seeks all civil remedies provided under the causes of action, including but not limited to compensatory, statutory, and/or punitive damages, and attorneys' fees and costs.

PARTIES

5. Plaintiff is a citizen of the Commonwealth of Massachusetts, and at all relevant times to this action, resided and was domiciled in Bristol County, Massachusetts. Plaintiff is a citizen of Massachusetts.

6. Defendant Goodyear Tire and Rubber Company is a corporation organized under the laws of Ohio, and its principal place of business is 200 Innovation Way, Akron, Ohio.

Defendant is a citizen of Ohio and is registered for service through Corporation Service Company, at 3366 Riverside Drive, Suite 103, Upper Arlington, Ohio, 43221.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class, including Plaintiff, is a citizen of a state different than Defendant.

8. This Court has personal jurisdiction over Defendant because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in Massachusetts. The privacy violations complained of herein resulted from Defendant's purposeful and tortious acts directed towards citizens of Massachusetts while they were located within Massachusetts. At all relevant times, Defendant knew that its practices would directly result in collection of information from Massachusetts citizens while those citizens browsed www.goodyear.com. Defendant chose to avail itself of the business opportunities of marketing and selling its goods and services in Massachusetts and collecting real-time data from website visit sessions initiated by citizens of Massachusetts while located in Massachusetts, and the claims alleged herein arise from those activities.

9. Goodyear also knows that many users visit and interact with Goodyear's websites while they are physically present in Massachusetts. Both desktop and mobile versions of Goodyear's website allow a user to search for nearby stores by providing the user's "current location," as furnished by the location-determining tools of the device the user is using or by the user's IP address (*i.e.*, without requiring the user to manually input an address). Users'

employment of automatic location services in this way means that Goodyear is continuously made aware that its website is being visited by people located in Massachusetts, and that such website visitors are being wiretapped in violation of Massachusetts statutory and common law.

10. Pursuant to 28 U.S.C. §1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

FACTUAL ALLEGATIONS

A. Website User and Usage Data Have Immense Economic Value

11. The "world's most valuable resource is no longer oil, but data."[1]

12. Earlier this year, Business News Daily reported that some businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, how consumers interact with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, data on consumer satisfaction) from consumers.[2] This information is valuable to companies because they can use this data to improve customer experiences, refine their marketing strategies, capture data to sell it, and even to secure more sensitive consumer data.[3]

13. In a consumer-driven world, the ability to capture and use customer data to shape products, solutions, and the buying experience is critically important to a business's success.

---

[1] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[2] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESS NEWS DAILY (Aug. 5, 2022; updated Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[3] *Id.*

Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[4]

14. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[5] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[6]

15. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [*i.e.*, $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[7]

B. Website Users Have a Reasonable Expectation of Privacy in Their Interactions with Websites

16. Consumers are skeptical and are wary about their data being collected. A report released by KPMG shows that "a full 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected."[8]

---

4 Brad Brown, Kumar Kanagasabai, Prashant Pant & Gonçalo Serpa Pinto, *Capturing value from your customer data*, MCKINSEY (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

5 *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, NO. 220 (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

6 *Id.* at 25.

7 *Id.*

8 Lance Whitney, *Data privacy is a growing concern for more consumers*, TECHREPUBLIC (Aug. 17, 2021), https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/.

17. Another recent paper also indicates that most website visitors will assume their detailed interactions with a website will only be used by the website and not be shared with a third-party they know nothing about.[9] As such, website visitors reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[10]

18. Privacy polls and studies show that a majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

19. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[11]

20. Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[12]

21. Users act consistently with their expectation of privacy. Following a new rollout of the iPhone operating software – which asks users for clear, affirmative consent before allowing

---

[9] *CUJO AI Recent Survey Reveals U.S. Internet Users' Expectations and Concerns Towards Privacy and Online Tracking*, CUJO AI (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.

[10] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, The Information Society, 38:4, 257, 258 (2022).

[11] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/.

[12] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER, (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

companies to track users – 85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[13]

C. How Session Replay Code Works

22. Session Replay Code, such as that implemented on www.goodyear.com, enables website operators to record, save, and replay website visitors' interactions with a given website. The clandestinely deployed code provides online marketers and website designers with insights into the user experience by recording website visitors "as they click, scroll, type or navigate across different web pages."[14]

23. While Session Replay Code is utilized by websites for some legitimate purposes, it goes well beyond normal website analytics when it comes to collecting the actual contents of communications between website visitors and websites. Unlike other online advertising tools, Session Replay Code allows a website to capture and record nearly every action a website visitor takes while visiting the website, including actions that reveal the visitor's personal or private sensitive data, sometimes even when the visitor does not intend to submit the data to the website operator, or has not finished submitting the data to the website operator.[15] As a result, website visitors "aren't just sharing data with the [web]site they're on . . . but also with an analytics service that may be watching over their shoulder."[16]

---

[13] Margaret Taylor, *How Apple screwed Facebook*, WIRED, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[14] Erin Gilliam Haije, *[Updated] Are session recording tools a risk to internet privacy?*, MOPINION (Mar. 7, 2018), https://mopinion.com/are-session-recording-tools-a-risk-to-internet-privacy/.

[15] *Id.*

[16] Eric Ravenscraft, *Almost Every Website You Visit Records Exactly How Your Mouse Moves*, MEDIUM (Feb. 5, 2020), https://onezero.medium.com/almost-every-website-you-visit-records-exactly-how-your-mouse-moves-4134cb1cc7a0.

24. Session Replay Code works by inserting computer code into the various event handling routines that web browsers use to receive input from users, thus intercepting the occurrence of actions the user takes. When a website delivers Session Replay Code to a user's browser, the browser will follow the code's instructions by sending responses in the form of "event" data to a designated third-party server. Typically, the server receiving the event data is controlled by the third-party entity that wrote the Session Replay Code, rather than the owner of the website where the code is installed.

25. The types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action, including all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through the website. To permit a reconstruction of a user's visit accurately, the Session Replay Code must be capable of capturing these events at hyper-frequent intervals, often just milliseconds apart. Events are typically accumulated and transmitted in blocks periodically throughout the user's website session, rather than after the user's visit to the website is completely finished.

26. Unless specifically masked through configurations chosen by the website owner, some visible contents of the website may also be transmitted to the Session Replay Provider.

27. Once the events from a user session have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video, meaning "[u]nlike typical analytics services that provide

aggregate statistics, these scripts are intended for the recording and playback of individual browsing sessions."[17]

28. Because most Session Replay Code will, by default, indiscriminately capture the maximum range of user-initiated events and content displayed by the website, researchers have found that a variety of highly sensitive information can be captured in event responses from website visitors, including medical conditions, credit card details, and other personal information displayed or entered on webpages.[18]

29. Most alarming, Session Replay Code may capture data that the user did not even intentionally transmit to a website during a visit, and then make that data available to website owners when they access the session replay through the Session Replay Provider. For example, if a user writes information into a text form field, but then chooses not to click a "submit" or "enter" button on the website, the Session Replay Code may nevertheless cause the non-submitted text to be sent to the designated event-response-receiving server before the user deletes the text or leaves the page. This information will then be viewable to the website owner when accessing the session replay through the Session Replay Provider.

30. Session Replay Code does not necessarily anonymize user sessions, either.

31. First, if a user's entry of personally identifying information is captured in an event response, that data will become known and visible to both the Session Replay Provider and the website owner.

---

[17] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, FREEDOM TO TINKER (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[18] *Id.*

32. Second, if a website displays user account information to a logged-in user, that content may be captured by Session Replay Code.

33. Third, some Session Replay Providers explicitly offer website owners cookie functionality that permits linking a session to an identified user, who may be personally identified if the website owner has associated the user with an email address or username.[19]

34. Session Replay Providers often create "fingerprints" that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. The resulting fingerprint, which is often unique to a user and rarely changes, is collected across all sites that the Session Replay Provider monitors.

35. When a user eventually identifies themselves to one of these websites (such as by filling in a form), the provider can then associate the fingerprint with the user identity and can then back-reference all of that user's other web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous – even if the user explicitly indicated that they would like to remain anonymous by enabling private browsing.

36. In addition to the privacy invasions caused by the diversion of user communications with websites to third-party Session Replay Providers, Session Replay Code also exposes website visitors to identity theft, online scams, and other privacy threats.[20] Indeed, "[t]he more copies of sensitive information that exist, the broader the attack surface, and when data is being collected . .

---

[19] *Id.*; *see also FS.identify – Identifying users*, FULLSTORY, https://help.fullstory.com/hc/en-us/articles/360020828113 (last visited Sep. 8, 2022).

[20] Juha Sarrinen, *Session replay is a major threat to privacy on the web*, ITNEWS (Nov. 16, 2017), https://www.itnews.com.au/news/session-replay-is-a-major-threat-to-privacy-on-the-web-477720.

. it may not be stored properly or have standard protections" increasing "the overall risk that data will someday publicly leak or be breached."[21]

37. Recognizing the privacy concerns posed by Session Replay Code, in 2019, Apple required app developers to remove or properly disclose the use of analytics code that allow app developers to record how a user interacts with their iPhone apps or face immediate removal from the app store.[22] In announcing this decision, Apple stated: "Protecting user privacy is paramount in the Apple ecosystem. Our App Store Review Guidelines require that apps request explicit user consent and provide a clear visual indication when recording, logging, or otherwise making a record of user activity."[23]

D. Goodyear Secretly Wiretaps its Website Visitors' Electronic Communications

38. Goodyear operates the website www.goodyear.com. Goodyear is an online and brick-and-mortar retailer and servicer for wheels, tires, and oil changes.

39. However, unbeknownst to the millions of individuals perusing Goodyear's products online, Goodyear intentionally procures and embeds Session Replay Code from Session Replay Providers on its website to track and analyze website user interactions with www.goodyear.com.

40. One such Session Replay Provider that Goodyear procures is Microsoft.

---

[21] Lily Hay Newman, *Covert 'Replay Sessions' Have Been Harvesting Passwords by Mistake*, WIRED (Feb. 26, 2018), https://www.wired.com/story/covert-replay-sessions-harvesting-passwords/.

[22] Zack Whittaker, *Apple tells app developers to disclose or remove screen recording code*, TECHCRUNCH (Feb. 7, 2019), https://techcrunch.com/2019/02/07/apple-glassbox-apps/.

[23] *Id.*

41. Microsoft is the owner and operator of a Session Replay Code titled Clarity, which provides basic information about website user sessions, interactions, and engagement, and breaks down users by device type, county, and other dimensions.[24]

42. Goodyear's procurement and use of Microsoft Clarity's Session Replay Code, and procurement and use of other Session Replay Code through various Session Replay Providers, is a wiretap in violation Massachusetts statutory law.

E. Plaintiff's and Class Members' Experience

43. While in Massachusetts, Plaintiff visited www.goodyear.com on his computer and cell phone to shop for tires in late 2021 and early 2022.

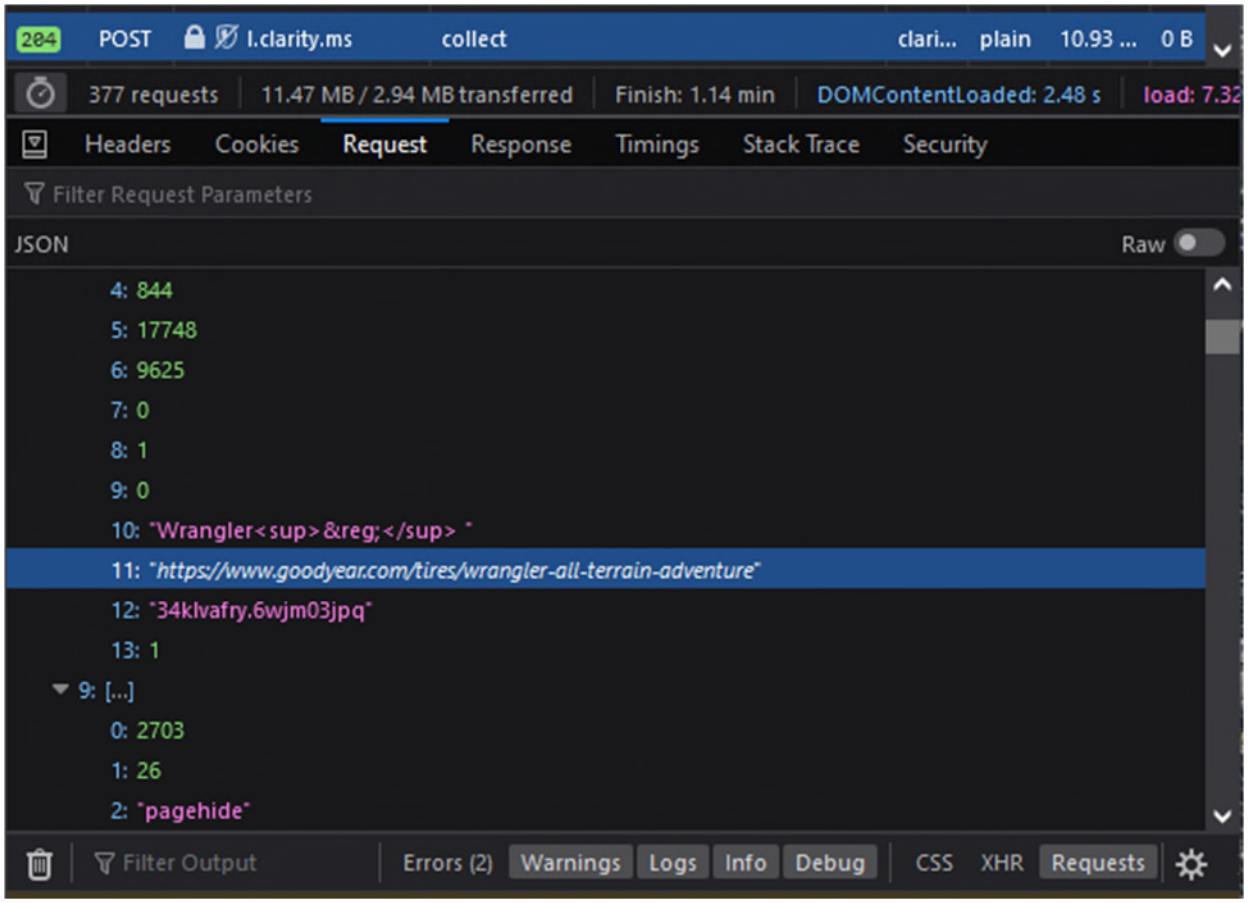
44. While visiting Goodyear's website, Plaintiff fell victim to Defendant's unlawful monitoring, recording, and collection of Plaintiff's Website Communications with www.goodyear.com.

45. Unknown to Plaintiff, Goodyear procures and embeds Session Replay Code on its website.

46. During the website visit, Plaintiff's Website Communications were captured by Session Replay Code and sent to various Session Replay Providers.

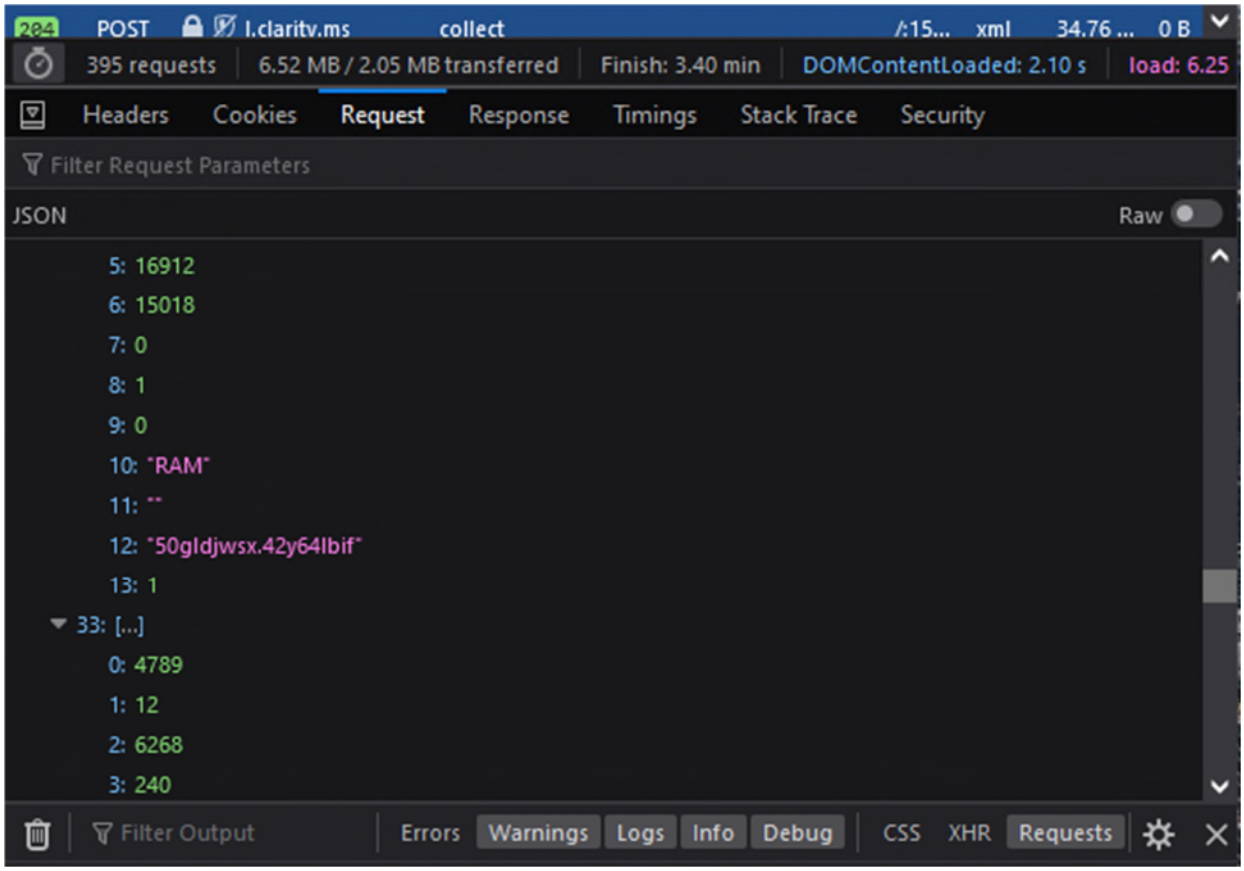
47. For example, when visiting www.goodyear.com, if a website user adds a product to their cart, that information is captured by the Session Replay Code embedded on the website:

[24] Jono Alderson, *An introduction to Microsoft Clarity*, Yoast (Nov. 11, 2020), https://yoast.com/introduction-microsoft-clarity/#h-what-is-microsoft-clarity.



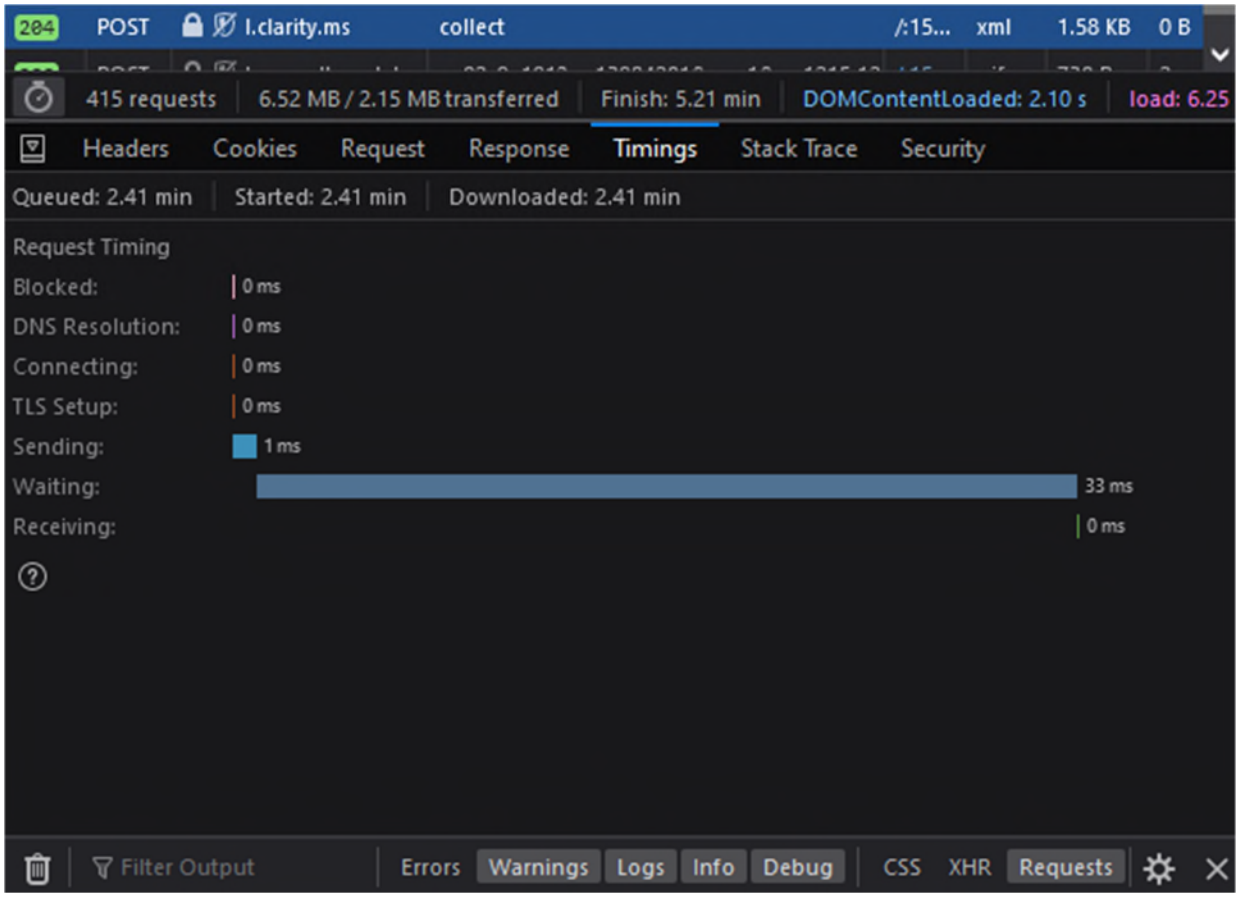
Depicting information sent to one of the Service Replay Providers – Microsoft – through a Service Replay Code – Clarity – after viewing "Goodyear Wrangler All-Terrain Adventure" tires while visiting www.goodyear.com.

48. Similarly, when entering in your vehicle information to view tires that fit your specific vehicle, that information is sent to Session Replay Providers:



Depicting information sent to one of the Service Replay Providers – Microsoft – through a Service Replay Code – Clarity – after selecting "RAM" as user vehicle make while visiting www.goodyear.com.

49. The wiretapping by the Session Replay Code is ongoing during the visit and intercepts the contents of these communications between Plaintiff and Goodyear with instantaneous transmissions to the Session Replay Provider, as illustrated below, in which only 34 milliseconds were required to send a packet of event response data, which would indicate whatever the website user had just done:



50. Session Replay Code operates in the same manner for all putative Class members.

51. Like Plaintiff, each Class member visited www.goodyear.com with Session Replay Code embedded in it, and the Session Replay Code intercepted the Class members' Website Communications with www.goodyear.com by sending hyper-frequent logs of those communications to Session Replay Providers.

52. Even if Goodyear masks certain elements when it configures the settings of the Session Replay Code embedded on its website, any operational iteration of the Session Replay Code will, by its very nature and purpose, intercept the contents of communications between the website's visitors and the website owner.

53. For example, even with heightened masking enabled, Session Replay Providers will still learn through the intercepted data exactly which pages a user navigates to, how the user moves

through the page (such as which areas the user zooms in on or interacted with), and additional substantive information.

54. As a specific example, if a user types a product into Goodyear's main search bar and initiates a search, even if the text entered into the search bar is masked, Session Replay Providers will still learn what is entered into the bar as soon as the search result page loads. This is so because the responsive search results will be displayed on the subsequent page, and the responsive content generated by Goodyear will repeat the searched information back on the generated page. That information will not be masked even if user-inputted text is fully masked in a text field.

CLASS ACTION ALLEGATIONS

55. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

Massachusetts Class:

All natural persons in Massachusetts whose Website Communications were captured in Massachusetts through the use of Session Replay Code embedded in www.goodyear.com.

56. Excluded from the Class are Defendant, its parents, subsidiaries, affiliates, officers, and directors, all persons who make a timely election to be excluded from the Class, the judge to whom this case is assigned, and any immediate family members thereof, and the attorneys who enter their appearance in this action.

57. **Numerosity:** The members of the Class are so numerous that individual joinder of all Class members is impracticable. The precise number of Class members and their identities may be obtained from the books and records of Goodyear or the Session Replay Providers.

58. **Commonality:** This action involves questions of law and fact that are common to the Class members. Such common questions include, but are not limited to: (a) whether Defendant procures Session Replay Providers to intercept Goodyear's website visitors' Website Communications; (b) whether Goodyear intentionally discloses the intercepted Website Communications of its website users; (c) whether Defendant acquires the contents of website users' Website Communications without their consent; (d) whether Defendant's conduct violates Massachusetts Wiretap Act, Mass. Gen. Laws ch. 272, §99; (e) whether Defendant's conduct violates Mass. Gen. Laws ch. 214, §1; (f) whether Plaintiff and the Class members are entitled to equitable relief; and (g) whether Plaintiff and the Class members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

59. **Typicality:** Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through the uniform prohibited conduct described above. For instance, Plaintiff and each member of the Class had their communications intercepted in violation of the law and their right to privacy. This uniform injury and the legal theories that underpin recovery make the claims of Plaintiff and the members of the Class typical of one another.

60. **Adequacy of Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do

so. Neither Plaintiff nor his counsel have any interest adverse to the interests of the other members of the Class.

61. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

62. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant intercepted Plaintiff's and Class members' Website Communications, then Plaintiff and each Class member suffered damages by that conduct.

63. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class members may be readily identified through Goodyear's books and records or the Session Replay Providers' books and records.

COUNT I
Violation of Massachusetts Wiretap Statute
(Mass. Gen. Laws ch. 272, §99)

64. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

65. Plaintiff brings this claim individually and on behalf of the Class.

66. The Massachusetts Wiretap Statute (the "Statute") prohibits the interception, use, or disclosure of any oral or wire communications which violates personal, property, or privacy interests. Mass. Gen. Laws ch. 272 §99(Q).

67. The express legislative purpose of Mass. Gen. Laws ch. 272, §99's unequivocal ban on secret recordings is to protect Massachusetts citizens' privacy. In fact, the statute's preamble states that secret recording "pose[s] grave dangers to the privacy of all citizens of the commonwealth." Mass. Gen. Laws ch. 272, §99 (A).

68. "Interception" means to "[S]ecretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication". Mass. Gen. Laws ch. 272, §99(B)(4).

69. "Intercepting device" means "any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and other than any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business." Mass. Gen. Laws ch. 272, §99(B)(3).

70. "Wire communication" means "***any communication*** made in whole or in part through the use of facilities for the transmission of communications by the ***aid of wire, cable, or other like connection*** between the point of origin and the point of reception". Mass. Gen. Laws ch. 272, §99(B)(1). [Emphasis added.]

71. "Contents" means "any wire or oral communication, means any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." Mass. Gen. Laws ch. 272, §99(B)(5).

72. "Person" means "any individual, partnership, association, joint stock company, trust, or corporation, whether or not any of the foregoing is an officer, agent, or employee of the United States, a state, or a political subdivision of a state." Mass. Gen. Laws ch. 272, §99(B)(13).

73. "Use" includes "willfully us[ing] or attempt[ing] to use the contents of any wire or oral communication, knowing that the information was obtained through interception[.]" Mass. Gen. Laws ch. 272, §99(C)(3)(b).

74. Goodyear is a person for purposes of the Act because it is a corporation.

75. Session Replay Code, like that procured by Goodyear, is an "intercepting device" used for the "capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and other than any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business." Mass. Gen. Laws ch. 272 §99(B)(3).

76. Plaintiff's and Class members' intercepted Website Communications constitute the "contents" of electronic communications within the meaning of the Act.

77. Goodyear intentionally procures and embeds Session Replay Code on its website to spy on, automatically and secretly, and intercept its website visitors' electronic interactions communications with Goodyear in real-time.

78. Plaintiff's and Class members' electronic communications are intercepted contemporaneously with their transmission.

79. Plaintiff and Class members did not consent to having their Website Communications wiretapped.

80. Any aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by this section or whose personal or property interests or privacy were violated by means of an interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications or who so violates his personal, property, or privacy interest, and shall be entitled to recover from any such person actual damages but not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1000, whichever is higher; punitive damages; and a reasonable attorney's fee and other litigation disbursements reasonably incurred. Mass. Gen. Laws ch. 272, §99(Q).

81. Goodyear's conduct violated Mass. Gen. Laws ch. 272, § 99 and therefore gives rise to a claim under Mass. Gen. Laws ch. 272, §99(Q).

82. Pursuant to Mass. Gen. Laws ch. 272, §99(Q) Plaintiff and the Class members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

83. Goodyear's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

COUNT II
Invasion of Privacy – Violation of Mass. Gen. Laws ch. 214, §1(B)

84. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

85. Plaintiff brings this claim individually and on behalf of the Class.

86. Pursuant to Mass. Gen. Laws ch. 214, §1., "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages."

87. Plaintiff and Class members have an objective, reasonable expectation of privacy in their Website Communications.

88. Plaintiff and Class members did not consent to, authorize, or know about Goodyear's intrusion at the time it occurred. Plaintiff and Class members never agreed that Goodyear could collect or disclose their Website Communications.

89. Plaintiff and Class members had an objective interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

90. Goodyear intentionally intrudes on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

91. Goodyear's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy.

92. Plaintiff and Class members were harmed by Goodyear's wrongful conduct as Goodyear's conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications and exposed Plaintiff and the Class to unwanted solicitation.

93. Goodyear's conduct has needlessly harmed Plaintiff and the Class by capturing intimately personal facts and data in the form of their Website Communications. This disclosure and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

94. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiff and Class members of the economic value of their interactions with Defendant's website, without providing proper consideration for Plaintiff's and Class members' property.

95. Further, Goodyear has improperly profited from its invasion of Plaintiff and Class members' privacy in its use of their data for its economic value.

96. As a direct and proximate result of Goodyear's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

97. Goodyear's conduct is ongoing, and it continues to unlawfully intercept the communications of Plaintiff and Class members any time they visit Defendant's website with Session Replay Code enabled without their consent. Plaintiff and Class members are entitled to declaratory and injunctive relief to prevent future interceptions of their communications.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of the other members of the proposed Class, respectfully request that the Court enter judgment in Plaintiff's and the Class's favor and against Defendant as follows:

A. Certifying the Class and appointing Plaintiff as the Class representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Declaring that Defendant's past conduct was unlawful, as alleged herein;

D. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;

E. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the Class, demands a trial by jury of any and all issues in this action so triable of right.

Dated: October 24, 2022

/s/ Joseph P. Guglielmo

Joseph P. Guglielmo BBO #671410
Carey Alexander
Ethan S. Binder
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Fl.
New York, NY 10169
Tel.: (212) 223-6444
jguglielmo@scott-scott.com
calexander@scott-scott.com
ebinder@scott-scott.com

Brian C. Gudmundson
Michael J. Laird
Rachel K. Tack

ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Tel.: (612) 341-0400
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.con
rachel.tack@zimmreed.com

Counsel for Plaintiff